

DOW JONES, A NEWS CORP COMPANY

DJIA **25964.82** -0.09% ▼S&P 500 **2901.52** 0.01% ▲Nasdaq **8109.54** 0.26% ▲U.S. 10 Yr **-1/32 Yield** 2.860% ▼Crude Oil **69.88** -0.53% ▼

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<https://www.wsj.com/articles/tech-support-scams-on-google-trigger-crackdown-1535755023>

TECH

Tech-Support Scams Prompt Google to Act

Wall Street Journal investigation finds fraudsters use Google search ads to masquerade as authorized service agents for companies such as Apple



Google headquarters in Mountain View, Calif. The company has instituted verification processes for some ads in the past.
PHOTO: DAVID PAUL MORRIS/BLOOMBERG NEWS

By *Samarth Bansal and Rob Barry*

Aug. 31, 2018 6:37 p.m. ET

Alphabet Inc.'s [GOOGL -1.80%](#) ▼ Google is taking action to weed out scam artists who advertise on its platform aiming to defraud customers seeking technical support online.

The move comes after a Wall Street Journal investigation found fraudsters were exploiting Google's advertising system by purchasing search ads and masquerading as authorized service agents for companies such as Apple Inc.

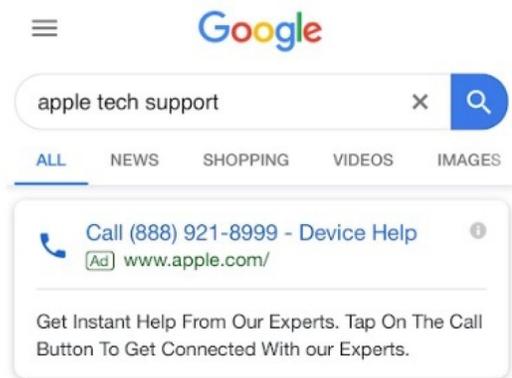
For instance, the first result in a recent Google search for the phrase "Apple tech support" showed a link to Apple.com and a toll-free number, with the suggestion: "Get instant help from our experts." The Journal found that the phone number didn't belong to Apple and instead led to a call center that engages in tech-support scams.

Responding to questions about the ads earlier this week, a Google spokeswoman told the Journal the company was committed to removing bad ads, and last year removed more than 100 such ads per second for violating company policies.

On Friday, Google announced a more stringent crackdown on tech-support ads. "We've seen a rise in misleading ad experiences stemming from third-party technical support providers and have decided to begin restricting ads in this category globally," Google's global product policy director David Graff said on the company's blog.

Google plans to roll out a verification program "to ensure that only legitimate providers of third-party tech support can use our platform to reach consumers," Mr. Graff wrote.

The company will start implementing the restriction on these ads immediately, but they will take weeks to go fully into effect in all languages and parts of the world, people familiar with the new policy said. They added that the verification process for allowing individual vendors back onto the platform is still being worked out.



This screenshot shows the first ad that appeared atop a recent Google search for 'apple tech support' featured Apple's web address, but clicking on the ad prompted the user to dial a number not affiliated with Apple. PHOTO: UNCREDITED

Google has instituted verification processes for other types of ads in the past, including local locksmith services and treatment centers, the people said. It has banned ads for bail-bond services and payday loans.

Technical scams have taken billions of dollars from unwitting Americans who handed over their payment information, according to government and industry experts. The issue is particularly acute for scams involving remote technical support, where users searching for computer help are sometimes shown deceptive ads and pop-up messages warning of virus infections.

A 2018 study found 72% of sponsored ads on major search engines related to technical support queries led to scam websites.

These scams are on the rise: Microsoft Corp., which receives around 12,000 complaints about tech support scams every month, reported a 24% increase in such complaints through 2017. The Federal Trade Commission registered 45,000 complaints about online tech support fraud in 2016, which the agency estimates is only a fraction of the true total.

The scams usually work this way: A person searching for tech help calls the number listed on an online ad. Once connected, the scammers ask for access to their victims' computers, where they run fake virus scanning software and fabricate security threats in an effort to convince users their computers are broken or compromised. Then, the scammers offer to sell what they claim are "support services," often at a cost of hundreds of dollars, the Journal found.

For instance, numerous ads appeared on Google's mobile website for search terms like "Apple help" showing what seemed to be official links to Apple's corporate website. But the ads actually lead to tech support scams that have no connection to Apple, the Journal found.

Apple didn't immediately respond to a request for comment.

When a Journal reporter identified himself and called the number displayed on a recent ad for the search term "Apple tech support," a man claiming to be an Apple engineer answered.

The man, who said his name was Sam Daniels, asked the reporter to log in to his email account. When the reporter did so, the man claimed to have been able to remotely monitor the computer via its IP address—a unique number used to identify computers on the internet.

"We have detected your IP address using your email ID and I can see your laptop is currently affected," he said, adding: "Hackers have put Trojan virus in your Apple device. Now, they will hack your email ID, Facebook ID and then your personal banking information."

The call was then transferred to another man who said his name was Mark Wallace and claimed to be an "antivirus hacking specialist." He too repeatedly claimed to work for Apple and said that hackers "can take all of your money with help of the IP address. They can also track your physical location."

To fix the purported problem, the second man asked the reporter to go to a nearby department store and buy a \$100 iTunes gift card. He asked the reporter to then share the alphanumeric code on the back of the card, which he described as an “antihacking card.”

“The amount is refundable,” he said.

When the reporter confronted him, he hung up with a final warning: “If anything happens to your account, Apple is not responsible.”

Independent experts say it isn’t possible to remotely access one computer or find its IP address by logging into email on another computer.

Write to Rob Barry at rob.barry@wsj.com

Appeared in the September 1, 2018, print edition as ‘Google Takes Aim At Tech-Help Scams.’

Copyright ©2017 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.